

REMARKS

Claims remaining in the present application are numbered 1-25. Claims 1, 9 and 17 have been amended. No new material has been added as a result of the above amendments to the Claims.

CLAIM REJECTIONS

35 U.S.C. § 112

The rejection states that Claim 1 recites the limitation "third values." The rejection further states that there is insufficient basis for limitation in the claim. The rejection further states that for the purposes of examination and from the specification stated by Applicant, the Examiner shall take the "third values" to be a third nonce or value generated or supplied from within the access point server.

Applicant respectfully expresses thanks to Examiner for the correct interpretation of the limitations within Claim 1, as well as within Claims 9 and 17 which contain similar limitations as presented Claim 1.

However, to more precisely point out and properly claim the inventive subject matter, Applicant has amended Claims 1, 9 and 17.

Therefore, currently amended Claims 1, 9, and 17 are now believed to particularly point and distinctly claim the subject matter Applicant regards as their invention. Accordingly,

Applicant respectfully asserts that currently amended Claims 1, 9 and 17 overcome the rejection under 35 U.S.C. § 112. As such Applicants respectfully request that the rejection of Claim 1, and Claims 9 and 17 under 35 U.S.C. § 112, be withdrawn and Claims 1, 9 and 17 be allowed.

35 U.S.C. § 103(a)

Claims 1-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over (Menezes et al, Handbook of Applied Cryptography) in view of (Schneier, Applied Cryptography) and Lincke et al, U.S. Patent No. 6,253,326. The rejection is respectfully traversed, for the reasons below. It is respectfully submitted that Claims 1-25 are patentable over Menezes in view of Schneier in view of Lincke.

Currently amended Claim 1 recites:

In a network access point, a method of processing encrypted communication, according to an encryption/decryption process, said method comprising:

receiving a first message from a wireless client, said first message comprising first values for a first random number and information identifying said wireless client and said access point and a first message authentication code of said information in said first message signed using a first signing key;

generating a second message comprising second values for a second random number and information identifying said access point and said wireless client and a second message authentication code of said information in said second message signed using a second signing key; and

sending said first values and said second values to an access point server, wherein said access point server generates a session key using said first values and said second values and also third values provided by said access point server, such that said processing is shared by said access point and said access point server.

The rejection states Menezes discloses, in pages 503-504 on Otway-Rees protocol, Handbook of Applied Cryptography, in a network access point, a method of processing encrypted communication, according to an encryption/decryption process in which the first wireless client in Alice, the first random number is the Nonce A, information identifying the client is her name, information identifying the access point is Bob, the message authentication code is an index number, and the message is signed message is the encryption by the key she shares with Trent and this message is received by Bob.

As understood by Applicant, Menezes may suggest (pages 503-504) Alice encrypts data for the server containing two nonces, N_a and M, and the identities of itself, Alice, and the party, Bob, to whom it wishes the server to distribute a key. Alice sends this and some plaintext to Bob. Thus, Applicants understand Menezes to disclose a message that contains a first and second nonce, N_a and M and an identifier for Alice and an identifier for Bob. As further understood by Applicant, Menezes suggests that the second random number M could be eliminated, or can be utilized solely as an administrative transaction identifier (12.30 Remark), such that if a previous communication had a transaction number of 112233, the subsequent transaction number might be 112234. The transaction number, as disclosed by Menezes (12.30 Remark), while considered desirable from an implementation standpoint, is considered dubious from a security standpoint.

However, Menezes, as understood by Applicant, does not teach or describe the limitations of Claim 1 which, in part, recites “and a first message authentication code of said information in said first message signed using a first signing key.” Thus, Applicant asserts that Menezes does not disclose the limitations of the first element in Claim 1, as recited.

The rejection further states Menezes discloses, in pages 503-504 on Otway-Rees protocol, Handbook of Applied Cryptography, a second message is generated by Bob, the second random number is Nonce B, information identifying the access point is Bob's name, information identifying the wireless client is Alice's name, the second message authentication code is an index number, and the message is signed or encrypted using another key, the one Bob shares with Trent.

As understood by Applicant, Menezes may suggest, in pages 503-504 on Otway-Rees protocol, Handbook of Applied Cryptography, a second message that contains its own nonce, N_b and an analogous encrypted message (with the same M, described by Menezes as an administrative transaction identifier) and this message along with Alice's message are to be sent to Trent.

However, Menezes, as understood by Applicant, does not teach or describe the limitations of Claim 1 which, in part, recites "and a second message authentication code of said information in said second message signed using a second signing key." Thus, Applicant asserts that Menezes does not disclose the limitations of the second element in Claim 1, as recited.

The rejection further states Menezes discloses, in pages 503-504 on Otway-Rees protocol, Handbook of Applied Cryptography, where the message generated by Alice and Bob are eventually sent to Trent, the access point server, where the first value is the random number of Alice, the second number is the random number of Bob. The session key is the session key generated by Trent, and the processing and decryption is shared between Bob and Trent.

As understood by Applicant, Menezes may suggest, in pages 503-504 on Otway-Rees protocol, Handbook of Applied Cryptography, Trent receives the message from Bob and uses the identifiers (M, Bob and Alice) to retrieve related symmetric keys K_{at} and K_{bt} then verifies the identifiers (M, Alice and Bob) match the recovered upon decrypting both parts of the message such that verifying M in particular confirms the encrypted parts are related.

However, Menezes, as understood by Applicant, does not teach or suggest the message received by Trent containing a first message authentication code of said information in said first message signed using a first signing key or a second message authentication code of said information in said second message signed using a second signing key nor does Menezes teach or describe the access point server (Trent) generating a session key using the first and second values in which the first value contains a first signing key and the second value contains a second signing key. Thus, Applicant asserts that Menezes does not disclose the limitations of the third element of Claim 1, as recited.

On page 4, the rejection concedes that Menezes fails to explicitly disclose using the first and second Nonce and generating a third value to be used in the generation of the session key. Moreover, Applicant respectfully submits that Menezes fails to teach or suggest this limitation.

On page 4, the rejection further concedes that Menezes fails to explicitly disclose the hardware embodiment where Alice is a wireless client, Bob is the access point and Trent is the access point server. Moreover, Applicant respectfully submits that Menezes fails to teach or suggest this limitation.

The rejection further states that key generation may employ any number of values. Schneier (page 175, "X9.17 key generation, Applied Cryptography) for example discloses X9.17 key generation which uses three different seeds for the generation of a key. Schneier (page 175, "X9.17 key generation, Applied Cryptography) further discloses that this method does not generate easy to remember keys, making it suitable for session keys.

Applicant wishes to respectfully point out that the above-cited reference (Schneier, page 175, "X9.17 key generation, Applied Cryptography) was not included with the cited references that accompanied the rejections. However, Applicant has obtained a copy of Schneier, page 175, "X9.17 key generation, Applied Cryptography.

As understood by Applicant, Schneier may suggest (page 175) X9.17, a standard specifying a method of key generation in which the key generation contains, in part, a timestamp T.

Applicant understands Menezes, page 503 of Otway-Rees, Handbook of Applied Cryptography to disclose the Otway-Rees protocol is a server-based protocol the same as Kerberos, but here without the requirement of timestamps.

Thus, Applicant respectfully asserts that combining the teachings of Schneier with the teachings of Menezes might have a detrimental effect to the functions desired by Menezes, as Menezes specifically does not require a timestamp. Thus, Applicant respectfully traverses the cited motivation to combine the teachings of Schneier with the teachings of Menezes.

The rejection further states that Lincke, et al, discloses (Figure 4) the use of a wireless client communicating with an access point which then in turn communicates with a server.

Lincke, as understood by Applicant, may suggest a wireless client communicating with an access point as well as a secure transaction (col. 84, line 48 to col. 90, line 3) between the wireless client and a proxy server in which the wireless client sends a message to the proxy server.

However, Lincke, as understood by Applicant, does not teach or describe a first message sent from a wireless client to a wireless access point, nor does Lincke teach or describe a first message authentication code of said information in said first message signed using a first signing key, nor does Lincke teach or describe a second message sent from the wireless access point or a second message authentication code of said information in said second message signed using a second signing key, nor does Lincke teach or describe the proxy server generating a session key predicated upon the values within the first and second messages. Further, as understood by Applicant, Lincke does not teach or describe transmitting a message from a proxy server to a wireless access point. Thus, Applicant respectfully asserts that Lincke does not remedy the shortcomings of Menezes.

Accordingly, Applicant asserts that Menezes and Schneier and Lincke, alone or in combination, do not teach the claimed limitations of Claim 1. Therefore, allowance of Claim 1 is earnestly solicited.

Claims 2-8 depend from Claim 1, which is believed to be allowable for the foregoing reasons. As such, it is respectfully submitted that Claim 1 and dependent claims 2-8 are patentable

over Menezes in view of Schneier in view of Lincke. As such, allowance of Claims 2-8 is respectfully solicited.

The rejection states that Claims 9-16 are substantially similar to Claims 1-8 and are rejected for the same reasons respectively.

For the reasons discussed in the response to Claim 1, neither Menezes nor Schneier nor Lincke, alone or in combination, teach or suggest the claimed limitations of Claim 9. Therefore, allowance of Claim 9 and dependent Claims 10-16 is earnestly solicited.

The rejection states that Claims 17-20 are substantially similar to Claims 1-4 and that Claims 22-25 are substantially similar to Claims 5-8 and are rejected for the same reasons respectively.

For the reasons discussed in the response to Claim 1, neither Menezes nor Schneier nor Lincke, alone or in combination, teach or suggest the claimed limitations of Claim 17. Therefore, allowance of Claim 17 and dependent Claims 18-25 is earnestly solicited.

CONCLUSION

For the above rationale, Applicants respectfully submit that the present invention as claimed is patentable over Menezes in view of Schneier in further view of Lincke under 35 U.S.C. § 103(a). As such, Applicants respectfully request that the rejections of Claims 1, 9 and 17 under 35 U.S.C. § 112 and the rejections of Claims 1-25 under 35 U.S.C. § 103(a) be withdrawn and Claims 1-25 be allowed.


Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

Please charge any additional fees or apply any credits to our PTO deposit account No. 23-0085.

Respectfully submitted,

Wagner, Murabito & Hao LLP

Dated: 5/5/, 2005



John P. Wagner
Registration No. 35,398

WAGNER, MURABITO & HAO LLP
Two North Market Street
Third Floor
San Jose, CA 95113
(408) 938-9060